



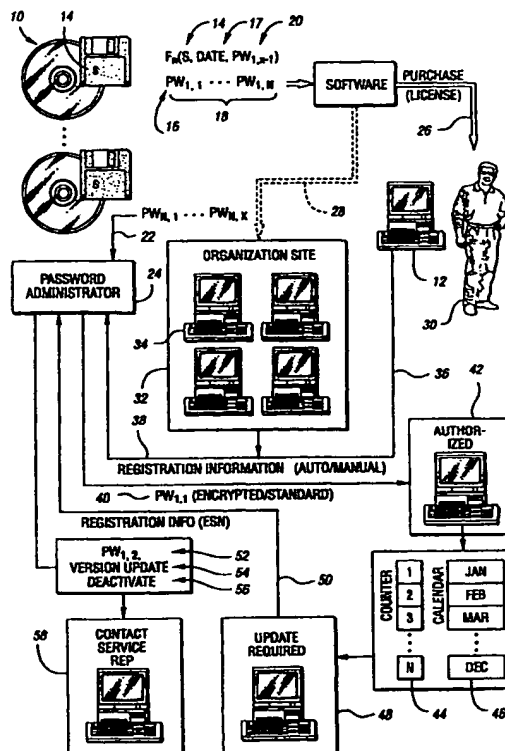
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : H04L 9/00, 9/06</p>	<p>A1</p>	<p>(11) International Publication Number: WO 99/63705</p> <p>(43) International Publication Date: 9 December 1999 (09.12.99)</p>
<p>(21) International Application Number: PCT/US99/11647</p> <p>(22) International Filing Date: 27 May 1999 (27.05.99)</p> <p>(30) Priority Data: 09/090,620 4 June 1998 (04.06.98) US</p> <p>(63) Related by Continuation (CON) or Continuation-in-Part (CIP) to Earlier Application US 09/090,620 (CON) Filed on 4 June 1998 (04.06.98)</p> <p>(71)(72) Applicant and Inventor: COLVIN, David, S. [US/US]; 3786 Ranya Drive, Commerce Township, MI 48382 (US).</p> <p>(74) Agents: BIR, David, S. et al.; Brooks &amp; Kushman, 22nd floor, 1000 Town Center, Southfield, MI 48075 (US).</p>		<p>(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).</p> <p>Published With international search report.</p>

**(54) Title: METHOD AND APPARATUS FOR SECURING SOFTWARE TO REDUCE UNAUTHORIZED USE**

**(57) Abstract**

A method and apparatus for securing software to reduce unauthorized use include associating a password (16) or series of passwords (18) with each copy or group of authorized software and requiring entry of a first password obtained from the developer or authorized representative (24) of the software after exchanging registration information (38). The method and apparatus may also require entry of a second password from the series associated with the software to continue using the software. A password (16) or authorization code series may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site (32). Preferably, subsequent passwords (16) or authorization codes are obtained from an authorized software developer (24), manufacturer, or distributor which gathers current information from the user (30) to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular. A code which disables the software may be communicated if the manufacturer determines that the user (30) is an unauthorized user.



**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece	ML	Mali	TR	Turkey
BG	Bulgaria	HU	Hungary	MN	Mongolia	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MR	Mauritania	UA	Ukraine
BR	Brazil	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Iceland	MX	Mexico	US	United States of America
CA	Canada	IT	Italy	NE	Niger	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NL	Netherlands	VN	Viet Nam
CG	Congo	KE	Kenya	NO	Norway	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NZ	New Zealand	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	PL	Poland		
CM	Cameroon	KR	Republic of Korea	PT	Portugal		
CN	China	KZ	Kazakstan	RO	Romania		
CU	Cuba	LC	Saint Lucia	RU	Russian Federation		
CZ	Czech Republic	LI	Liechtenstein	SD	Sudan		
DE	Germany	LK	Sri Lanka	SE	Sweden		
DK	Denmark	LR	Liberia	SG	Singapore		
EE	Estonia						

-1-

METHOD AND APPARATUS FOR SECURING  
SOFTWARE TO REDUCE UNAUTHORIZED USE

Technical Field

5       The present invention relates to apparatus and  
methods for reducing unauthorized use of software.

Background Art

10       Software developers are often victims of  
illicit copying and unauthorized use of their software  
in violation of contractual obligations imposed by  
licensing agreements and subject to civil and criminal  
penalties under various domestic and foreign laws.  
Unauthorized entities range from a relatively small  
percentage of the total users to an overwhelming  
majority of illegal users. Such unauthorized use not  
15       only amounts to theft of the developers' intellectual  
property, but also reduces the number of programs sold  
and therefore the associated profitability of the  
developer. This may ultimately diminish the creative  
effort expended by the software developers due to the  
20       reduced financial incentive. The advent of the internet  
has contributed to the proliferation of pirated  
software, known as "warez", which is easily located and  
readily downloaded.

25       Various strategies have been employed to make  
unauthorized duplication and use of software more  
difficult. One such approach is to provide a hardware  
"key" which is typically installed in the parallel port .

-2-

of the computer to provide a software interlock. If the key is not in place, the software will not execute. This method is relatively expensive for the developer and cumbersome for the authorized user while remaining  
5 vulnerable to theft by duplication of the hardware key.

Another approach requires the user to enter a serial number or customer identification number during installation of the software. Missing or invalid registration information prevents installation of the  
10 software. This approach is easily defeated by transferring the serial number or customer identification number to one or more unauthorized users.

Yet another approach requires registering the software with the manufacturer or distributor to obtain  
15 an operational code or password necessary for installation of the software. Again, once the operational code or password is obtained, it may be perpetually transferred along with pirated copies to numerous unauthorized users.

Various copy protection strategies have been employed to reduce the number of unauthorized copies available. This approach is generally disfavored by  
20 users who may have a legitimate need to make backup or archival copies or transfer a copy to a new computer or hard drive.  
25

While prior art strategies have enjoyed various levels of success in reducing unauthorized use of software, they often impose a significant burden on the authorized users or are easily defeated by  
30 unauthorized users. As such, software developers need an apparatus and/or method for reducing unauthorized use.

-3-

of software which does not burden the authorized users to dissuade them from purchasing and using the protected software.

### Summary Of The Invention

5                   Thus, one object of the present invention is to provide an apparatus and method for improving software security throughout the lifetime of the software.

10                   Another object of the present invention is to provide an apparatus and method for monitoring the number of users of a software product, both authorized and unauthorized.

15                   Yet another object of the present invention is to provide an apparatus and method for the software manufacturer to maintain contact with the user over an extended period of time.

20                   A further object of the present invention is to provide a method and apparatus for reducing unauthorized use of software which facilitate periodic software updates and forwarding of information, when and if desired.

25                   A still further object of the present invention is to identify those entities responsible for unauthorized copying or use of software so that appropriate action may be taken, such as disabling the software, requesting payment from the user, or seeking civil or criminal penalties.

-4-

Another object of the present invention is to provide a method and apparatus for reducing unauthorized software use which deactivates unauthorized copies when an unauthorized user attempts to obtain a password.

5           In carrying out the above objects and other objects, features, and advantages of the present invention, a method for securing software includes associating a series of passwords or authorization codes with each copy or group of authorized software,  
10           requiring entry of a first password from the series associated with the software upon first use of the software, and subsequently requiring entry of a second password from the series associated with the software to continue using the software. A password or  
15           authorization code series may be associated with each authorized copy or with a group of copies such as those distributed to a particular organization or site. Preferably, subsequent passwords or authorization codes are obtained from an authorized software developer,  
20           manufacturer, or distributor which gathers current information from the user to monitor compliance with licensing restrictions. The number and frequency of required password updates may be regular or irregular depending upon the application, user, or software  
25           manufacturer.

          The present invention contemplates, but does not require, more frequent password updates for more complex software because it is generally more costly to  
30           develop (and therefore more valuable to users) whereas less costly software would require fewer password updates to reduce administrative costs associated with password maintenance.

-5-

Password or authorization code updates may be obtained automatically or manually. Automatic updates are accomplished using electronic communication between the manufacturer's computer (or an authorized representative) and the user's computer. Updates may be performed by a direct modem connection, via email, a web browser, or the like. The particular time and nature of updates and the user interface utilized to implement the updates may vary by manufacturer or product. Manual updates are performed by advance or periodic notifications generated by the software to alert the user that password updates are required or will be required in the near future. The user may then contact the manufacturer for the specific password update via telephone, mail, email, or the like. Password advisories normally occur prior to the periodic termination of the operating period which may be measured by program starts, elapsed running time, calendar period, etc. Password updates may be in the form of alphanumeric and/or encrypted passwords or of any other conventional type.

Preferably, the user must provide registration information prior to receiving the original or updated password or authorization code. Registration information may be entered by the user or automatically acquired (and transmitted for automatic updates) by the software. Registration information may include a serial number, registration number, TCP/IP address, user name, telephone number, computer specific information, etc. This information may be encoded and/or encrypted to make it less susceptible to tampering by unauthorized users. The registration information is preferably monitored and compared to previously captured information to control the number of authorized copies of software and/or.

-6-

identify unauthorized users. If unauthorized use is suspected, a password or authorization code may be provided which subsequently disables the software, either immediately or after some period of time so that  
5 an authorized user is provided an opportunity to rectify the information which caused deactivation.

A number of advantages result from various implementations of the present invention. For example, the present invention reduces unauthorized use of  
10 software without imposing a significant burden on authorized users. The present invention controls the number of copies of authorized software by monitoring registration information and deactivation of suspected pirated copies. Requiring authorized users to  
15 periodically update a password or authorization code provided by a password administrator improves accuracy of contact information for marketing related products and distribution of product updates. The present invention also provides a variable level of software  
20 security which can be tailored to the particular application depending upon the value of the application to potential software pirates.

The above advantages and other advantages, objects, and features of the present invention will be  
25 readily apparent from the following detailed description of the best mode for carrying out the invention when taken in connection with the accompanying drawings.

#### **Brief Description Of The Drawings**

Fig. 1 is a block diagram illustrating various  
30 features of a method and apparatus for securing software according to the present invention;



-7-

Fig. 2 is a flow diagram illustrating generally a method for securing software according to the present invention; and

5 Fig. 3 is a more detailed flow diagram illustrating representative embodiments of a method and apparatus for securing software according to the present invention.

**Best Mode(s) For Carrying Out The Invention**

10 Referring now to Fig. 1, a block diagram illustrating various features of a method and apparatus for securing software according to the present invention is shown. Manufacturers or developers create application programs or software which is stored in the form of data representing program instructions  
15 executable by a computer on computer readable media 10. Computer readable media 10 may include any medium capable of storing such instructions which is directly or indirectly readable by a computer, such as computer  
20 12. Computer readable media may include floppy disks, hard drives, CD-ROMs, floptical disks, magnetic tape, and the like. Each copy or group of copies of the software may have an associated serial number, indicated generally by reference numeral 14, and an associated  
25 password 16 which may be one of a series of associated passwords 18 as explained in greater detail below. Each password 16 may be an alphanumeric character string which may be encoded or encrypted or a binary or hexadecimal machine readable string to resist tampering by unauthorized users. Passwords 16 within series 18  
30 may be randomly assigned or may be generated using a suitable algorithm, many of which are known in the art. Likewise, passwords 16 may be based on serial number 14,

-8-

a current date or version date 17, and/or a previous password 20 from the series of passwords.

After the password or passwords are created and associated with one or more serial numbers or copies of the software, they may be transferred to an authorized representative of the software, as represented by arrow 22, such as a password administrator 24. Of course, the original manufacturer or developer of the software may also function as password administrator 24. The software may be distributed by purchase or more commonly it is licensed as represented by arrows 26 and 28 to individuals 30 and groups 32, respectively. Preferably, the software is distributed to the end users without its associated password 16 which must be obtained from password administrator 24. Alternatively, computer readable media 10 may be distributed with the first password 16 of a series of passwords 18. Each authorized user preferably has software with a unique identifier, such as a serial number, whether the authorized user is an individual, such as user 30, or a group or region, indicated generally by reference numeral 32. However, the same password or series of passwords may be associated with a number of serial numbers to reduce the administrative burden for password administrator 24. For example, each end user 34 associated with organization or site 32 may have the same password or series of passwords. Preferably, not more than one password is distributed with each authorized copy so that the end users will need to contact password administrator 24 to obtain additional passwords for continued use of the software as explained in greater detail below.

-9-

During the initial use or installation of the software on computers 12,34, a password or authorization code will be required by the software to function properly. The end user must contact the authorized representative for the software, such as password administrator 24, to obtain the appropriate authorization code or password as indicated generally by arrows 36. Password administrator 24 obtains registration information 38 from the end user and provides an appropriate password or authorization code to the software as indicated by reference numeral 40. Communication of registration information and the authorization code may be accomplished either manually or automatically depending upon the particular application and configuration of the software. Manual communication may be by email, regular mail, telephone, automated voice response system, web browser, direct modem transfer, or the like but requires a varying level of intervention by the end user depending upon the particular type of communication. Automatic communication may use similar methods or means to communicate the information but is performed without user intervention, although the user may be advised or notified that the process is occurring or has occurred.

Registration information 38 may include traditional contact information, such as name, address, email, phone, etc. but preferably includes information which can be obtained without intervention by the end user to improve its veracity. Such information may include identification of a TCP/IP address, originating telephone number, or computer-specific information associated with the end user. Computer-specific information may include an electronic serial number (ESN) which uniquely characterizes the hardware.

-10-

configuration of the computer based on information stored in the computer's non-volatile CMOS, registry, motherboard serial number, or the like. Password administrator 24 preferably stores the registration information to be used for various purposes according to the present invention to reduce unauthorized use of software. For example, password administrator 24 may use the registration information to monitor compliance with licensing terms by determining whether a particular serial number has been installed on more than one computer or by more than one end user. Administrator 24 may compare the registration information with previously received registration information to determine whether to issue an authorization code or password, or to provide a code which disables further operation of the software. The registration information may also be used to contact the end users for marketing new products or versions, or providing software updates.

The password or authorization code is communicated to the software as represented by reference numeral 40. Depending upon the particular implementation, the password may be provided to the end user who manually enters the information into the computer 42 to begin or continue using the software. The password or authorization code may be encoded as an alphanumeric string using various numbers and letters which represent meaningful information to the administrator but appear to be randomly generated to the end user. Alternatively, an encryption algorithm may be used to transmit the information. Preferably, the password authorizes the software to execute on computer 42 for a first predetermined period as represented by counter 44 or calendar 46. The predetermined period may vary based on the particular authorized user, the cost .

-11-

of the software, the number of estimated unauthorized copies, etc. For example, it is anticipated that more expensive software would provide a shorter period of authorization to provide a higher level of security.

5 The higher revenue generated by the software offsets any increased administrative expense of password administrator 24 due to the increased frequency of updates required.

As indicated by counter 44 and calendar 46,

10 the authorized period of use may be measured either in calendar days (months, years, etc.) or in execution hours, number of accesses, or the like. Once the authorized period expires, the software requires a new password or authorization code as indicated by reference

15 numeral 48. This may be accomplished automatically and transparently to the end user by electronically contacting password administrator 24 and exchanging current registration information 50. Administrator 24 may compare the current registration information 50 with

20 previously received registration information to determine if at least a portion of the information matches for that particular serial number or group of serial numbers. This comparison may be used to determine whether the end user is an authorized user or

25 an unauthorized user.

The information provided to the software by administrator 24 may depend upon whether the user is determined to be authorized or unauthorized. For example, if the user is determined to be an authorized

30 user, a subsequent password 52 from the series of passwords associated with the software serial number or group may be communicated which authorizes the software for an additional operation period. As the software

-12-

becomes less valuable, such as when new versions are released, the authorization period may increase and preferably eventually allows indefinite use of the software. Of course, an exceedingly long period (10  
5 years for example) may be essentially equivalent to an indefinite period of operation. In addition to a subsequent password, an updated version 54 of the software may be transferred or offered to the end user. If the user is determined to be an unauthorized user, an  
10 appropriate message may be transmitted to alert the user to a discrepancy in the registration information, and the operational password may be withheld. Alternatively or in addition, a code 56 which deactivates the software may be communicated. As another alternative, a  
15 shortened authorization period may be provided along with a password and a message which indicates the end user must contact administrator 24 or another customer service representative to verify the user's status as represented by reference numeral 58. In the event the  
20 user is determined to be unauthorized, password administrator 24 may decline to download a password at which time the software may automatically become inoperative after the current operational period has lapsed.

25 Referring now to Fig. 2, a flow diagram generally illustrating a method for securing software according to the present invention is shown. A password or series of passwords is associated with a particular copy or group of copies of software prior to  
30 distribution (without the password or with only one of a series of passwords) as represented by block 80. A series of passwords may be associated with the software using an appropriate password generation algorithm with parameters which vary based on the particular copy. For.

-13-

example, a algorithm or mathematical equation or formula may be used to generate passwords with one or more of the parameters of the equation corresponding to letters or characters in the serial number of the software.

5           For applications which have only a single password for each copy or group of copies, the password may not be distributed with the software so the end user must contact the developer or authorized representative as represented by block 82. For applications with two  
10 or more passwords, an initial password may be provided or the software may operate without a password for a first period to provide ample opportunity for the end user to acquire the initial/subsequent password. Registration information may be required as a  
15 precondition to providing a valid authorization code or password. This allows the developer or authorized representative to monitor compliance with licensing terms and/or take appropriate action for unauthorized users.

20           The password or authorization code is communicated to the software as represented by block 84 to make the software operational on the end user's computer. This may be performed automatically, without user intervention, or manually when initiated by the  
25 user using various communication channels, such as regular mail, email, web browser, direct modem connection, etc. The method may optionally require periodic updates at regular, irregular, or random intervals based on elapsed running time, calendar time,  
30 or the like, as represented by block 86. The software may prompt the user when the end of the authorization period is approaching to provide an opportunity to obtain a subsequent authorization code for continued use.

-14-

of the software.

Referring now to Fig. 3, a more detailed flow diagram illustrating a method and/or apparatus for securing software according to the present invention is shown. The software manufacturer or developer (source) produces software which requires initial and/or periodic password updates to become or to remain operational as depicted in box 112. Software may be associated with individual end users, a regional (geographic) or other group of users, or users associated with a particular organization or site. Providing passwords or authorization codes for groups rather than each individual significantly reduces the number of passwords required and the corresponding administrative overhead including electronic storage and transmission requirements.

Following production by the software manufacturer, the source electronically stores the password information for future transmission to the user as shown in box 114. The password information may be the actual passwords or information used to generate subsequent passwords based on the individual copy or group of copies of the software. The embodiment depicted in Fig. 3 is intended to interlock specific pieces or groups of software with corresponding passwords or authorization codes.

Once the software is acquired by the user 116, the user installs (partially or fully) the software in his computer or computer network 118. Following installation of the software, the user is prompted to register the software and obtain the necessary



-15-

operational password which may be an alphanumeric string which is encoded or encrypted, or a binary (machine readable) code. The user is allowed to choose between automatic or manual registration 120. If automatic  
5 registration is selected 122, the program automatically contacts the source via a modem or other connection to obtain the operational password following registration 124.

Once contacted, the source searches for  
10 previous registration of the software with the registration number or user identification 126. If the software has not been previously registered 128, the source transmits the necessary password 130 wherein the software becomes operational 134. If registration  
15 information has been previously entered and does not match the current registration information, the source notifies the user of a previous registration of the same software 132 and thereafter takes appropriate action 136. Such action can either include denying the  
20 necessary operational password 138, continuing the password download if the source desires 130 or other appropriate action or actions.

Following the initial registration of the software and downloading of the first operational  
25 password, the software remains operational for a given interval which may be an operation period or time period (random, regular, or irregular). Once the first interval expires, the program notifies the user of the necessity to obtain the next operating password 140.  
30 The user's computer contacts the source via modem 142 and the source determines if previous inquiries have

-16-

been made for the same user 144 based on the registration information. These step(s) may be fully automated, thereby eliminating the need for user intervention or notifying the user.

5                   The source either transmits the password 148 or notifies the user of a duplicate inquiry 149. If a duplicate inquiry has been made, the source either declines to download 150 the password so that the software becomes non-operational 152 after the current  
10                   operational period elapses or the source transmits the password 148 if desired. During any of the contact periods between the source and the user, the source may elect to download software updates or additional information 154. Following the downloading or the  
15                   necessary operational password, the software becomes or remains operational 156. This sequence is selectively repeated 158 as determined by the authorization interval selected by the source and communicated to the software.

                  As shown in Fig. 3, the user may have the  
20                   option of manual registration 160 and password input as opposed to automatic registration. Alternatively, the source may require manual registration to verify the accuracy of at least some of the registration information since it will be used to send the  
25                   authorization code or password to the user. If the user provides inaccurate information, the password will not be transmitted and the software will not be operational. After initial registration, optionally the user may elect to convert to automatic electronic contact at any  
30                   time. Where manual registration is selected 160 (or required), the user contacts the source via telephone,

-17-

mail, email, internet, or the like to obtain the operational password following registration 162.

Once contacted, the source searches for previous registration of the software with the same serial number, registration number or user identification 164. If the software has not been previously registered 166, the source transmits the necessary password 168 wherein the software becomes operational 172. If a duplicate registration occurs, the source notifies the user of a previous registration of the same software 170 and thereafter takes appropriate action 174. Such action can either include not providing the necessary operational password 176 or continuing the password transmission if the source desires 168.

Following the initial registration of the software and transmission of the first operational password, the software remains operational for a given operation interval after which the software notifies the user of the necessity to obtain the next operating password 178. The user contacts the source via telephone or by mail 182 and the source determines if previous inquiries have been made for the same user 184. The user may elect to convert to automatic electronic registration during this period 180, however, this step is optional.

The source either transmits the password 188 or notifies the user of a duplicate inquiry 190. If a duplicate inquiry has been made, the source either

-18-

declines to download the password 196 (after which the software becomes non-operational 198) or the source transmits the password 188 if desired. During any of the contact periods between the source and the user, the source may elect to transmit software updates or additional information 192. Following the downloading or the necessary operational password the software becomes or remains operational 194. The sequence for successive operation intervals may then be repeated at the source's discretion 200.

It is understood that the representative methods of the present invention do not need to continue after initial registration and password transmission. Likewise, the process may be discontinued at some point in time by downloading a lifetime password which authorizes the software indefinitely. For example, this may be desirable after the software is deemed obsolete. It is further understood that the specific sequencing of events is not necessary for the proper implementation of the present invention. The invention further allows for compatibility with existing software or other security measures.

While the best modes for carrying out the invention have been described in detail, those familiar with the art to which this invention relates will recognize various alternative methods for carrying out the invention as described by the following claims.

-19-

What Is Claimed Is:

1. A method for securing software to reduce unauthorized use of the software, the method comprising:  
requiring entry of a first password upon first  
5 use of the software; and  
subsequently requiring entry of another password to continue using the software.
2. The method of claim 1 further comprising:  
associating a series of passwords with the  
10 software for each authorized user prior to distribution of the software.
3. The method of claim 2 wherein the authorized user is a group having a separate copy of the software for each of at least two end users.
- 15 4. The method of claim 1 further comprising including not more than one of the passwords with the software for distribution to each authorized user.
5. The method of claim 1 further comprising obtaining at least one password from an authorized  
20 representative of the software.
6. The method of claim 5 wherein the step of obtaining comprises electronically communicating with the authorized representative.
7. The method of claim 1 further comprising  
25 periodically repeating the step of subsequently requiring entry of another password for continued operation of the software.

-20-

8. The method of claim 1 further comprising repeating the step of subsequently requiring entry of another password at regular intervals.

5           9. The method of claim 1 further comprising:  
          requiring communication of registration  
information associated with the end user to an  
authorized representative of the software prior to  
communicating the password to the software.

10          10. A method of securing software to reduce  
unauthorized use, the method comprising:

          associating a password with the software, the  
password not being distributed concurrently with the  
software;

15          requiring an end user to contact a  
representative to obtain a password previously  
associated with the software; and

          communicating a password previously associated  
with the software to the software, wherein the software  
is not functional until the password has been  
20       communicated.

11. The method of claim 10 wherein the step  
of communicating comprises electronically communicating  
the password.

25          12. The method of claim 10 wherein the step  
of communicating is performed automatically by the  
software and the authorized representative.

13.       The method of claim 10 further  
comprising:  
          obtaining registration information associated  
30       with the end user as a precondition for performing the.

-21-

step of communicating the password.

14. The method of claim 13 wherein the step of obtaining registration information is performed substantially simultaneously with the step of communicating the password.

15. The method of claim 13 wherein the step of obtaining registration information comprises obtaining registration information from a computer on which the software has been installed.

16. The method of claim 10 further comprising:  
obtaining registration information associated with the end user; and  
encoding the registration information so it is not readily discernible.

17. The method of claim 10 wherein the step of communicating comprises communicating the password to the end user enabling the end user to supply the password to the software.

18. The method of claim 10 wherein the step of associating a password comprises associating a series of passwords with the software.

19. The method of claim 18 further comprising:  
periodically requiring a new password, the new password being obtained from the series of passwords previously associated with the software.

20. The method of claim 19 wherein the step

-22-

of periodically requiring a new password is performed at regular intervals.

21. The method of claim 19 wherein the step of periodically requiring a new password is performed at intervals based on elapsed execution time of the software.

22. The method of claim 19 wherein the step of periodically requiring a new password is performed at intervals based on elapsed time.

23. The method of claim 19 wherein the step of periodically requiring a new password is performed at predetermined intervals.

24. The method of claim 18 further comprising:  
periodically requiring registration information associated with the end user to obtain a new password, the new password being obtained from the series of passwords previously associated with the software.

25. The method of claim 24 further comprising:  
comparing the registration information with previously obtained registration information associated with the software to determine whether the end user is an authorized user.

26. The method of claim 25 further comprising:  
providing a new password only if at least a portion of the registration information matches.



-23-

previously obtained registration information.

27. The method of claim 10 further comprising:

5 periodically requiring a new password for continued operation of the software, the new password being obtained from the representative.

28. The method of claim 10 further comprising:

10 periodically requiring a new password for continued operation of the software, the new password being obtained from the representative after providing registration information associated with the end user;

comparing the registration information with previously obtained registration information;

15 providing a new password which allows continued operation of the software if the step of comparing indicates the end user is an authorized user; and

20 providing a new password which disables the software if the step of comparing indicates the end user is an unauthorized user.

29. The method of claim 10 further comprising:

25 obtaining registration information associated with the end user as a precondition for performing the step of communicating the password; and

modifying the password based on the registration information.

30. The method of claim 10 further comprising  
30 determining a new password using a previous password.

-24-

31. A computer readable storage medium having data stored therein representing software executable by a computer, the software including instructions to reduce use of the software by unauthorized users, the  
5 storage medium comprising:

instructions for requiring an end user to contact an authorized representative to obtain a password associated with the software; and

10 instructions for disabling the software until the password has been communicated to the software.

32. The computer readable storage medium of claim 31 further comprising:

instructions for obtaining registration information associated with the end user.

15 33. The computer readable storage medium of claim 31 further comprising:

instructions for periodically requiring entry of a new password for continued operation of the software.

20 34. The computer readable storage medium of claim 33 further comprising:

instructions for disabling the software after a predetermined password is communicated to the software.

25 35. The computer readable storage medium of claim 33 further comprising:

instructions for automatically contacting an authorized representative of the software to communicate registration information and obtaining authorization for  
30 continued operation of the software.

-25-

36. The computer readable storage medium of claim 35 further comprising:

instructions for encoding the registration information.

5           37. A method of securing software to reduce use of the software by unauthorized users, the method comprising:

associating a series of passwords with each unit of software;

10           requiring communication of registration information to an authorized representative for the software to receive a first password from the series of passwords associated with the software, the registration information being associated with an end user of the  
15           software;

periodically repeating the step of requiring communication of registration information to obtain a subsequent password from the series of passwords for continued operation of the software.

20           38. A method of securing software to reduce unauthorized use of the software, the method comprising requiring communication of registration information associated with a user of the software to obtain a password which enables operation of the software.

25           39. A method of securing software to reduce unauthorized use of the software, the method comprising requiring periodic communication of registration information associated with a user of the software to obtain a password which enables continued operation of  
30           the software.

-26-

40. A method for reducing unauthorized use of software, the method comprising:

requiring an end user to contact an authorized representative of the software upon initial use of the software by the end user;

communicating registration information associated with the end user to the authorized representative; and

disabling the software if the registration information indicates that the end user is an unauthorized user.

41. A method for reducing unauthorized use of software, the method comprising:

requiring registration information to be entered during initial use of the software;

communicating the registration information to an authorized representative of the software;

determining whether the software has been previously registered;

if the software has been previously registered, determining whether the registration information matches at least a portion of the previous registration information;

communicating an authorization code to the software upon receiving the registration information if the software has not been previously registered or if the registration information matches at least a portion of the previous registration information, the authorization code allowing continued operation of the software for a first predetermined period;

after the first predetermined period has expired, requiring a subsequent authorization code for continued operation of the software, the subsequent authorization code being communicated only if.

-27-

registration information indicates the end user is an authorized user based on previously received registration information.

5           42. A method of securing software to reduce unauthorized use, the method comprising:

          associating a plurality of passwords with the software and distributing one of the plurality of passwords concurrently with the software;

10           requiring an end user to contact a representative another one of the passwords previously associated with the software; and

          communicating one of the passwords previously associated with the software to the software, wherein the software remains functional only until the password  
15 expires.

          43. The method of claim 42 wherein the step of communicating comprises electronically communicating the password.

20           44. The method of claim 42 wherein the step of communicating is performed automatically by the software and the representative.

          45. The method of claim 42 further comprising:

25           obtaining registration information associated with the end user as a precondition for performing the step of communicating the password.

          46. The method of claim 42 further comprising:

30           periodically requiring a new password for continued operation of the software, the new password.

-28-

being obtained from the representative.

47. The method of claim 42 further comprising:

- 5 periodically requiring a new password for continued operation of the software, the new password being obtained from the representative after providing registration information associated with the end user;
- 10 comparing the registration information with previously obtained registration information;
- providing a new password which allows continued operation of the software if the step of comparing indicates the end user is an authorized user; and
- 15 providing a new password which disables the software if the step of comparing indicates the end user is an unauthorized user.

48. The method of claim 42 further comprising:

- 20 obtaining registration information associated with the end user as a precondition for performing the step of communicating the password; and
- modifying the password based on the registration information.

49. The method of claim 42 further comprising
- 25 determining a new password using a previous password.

1/6

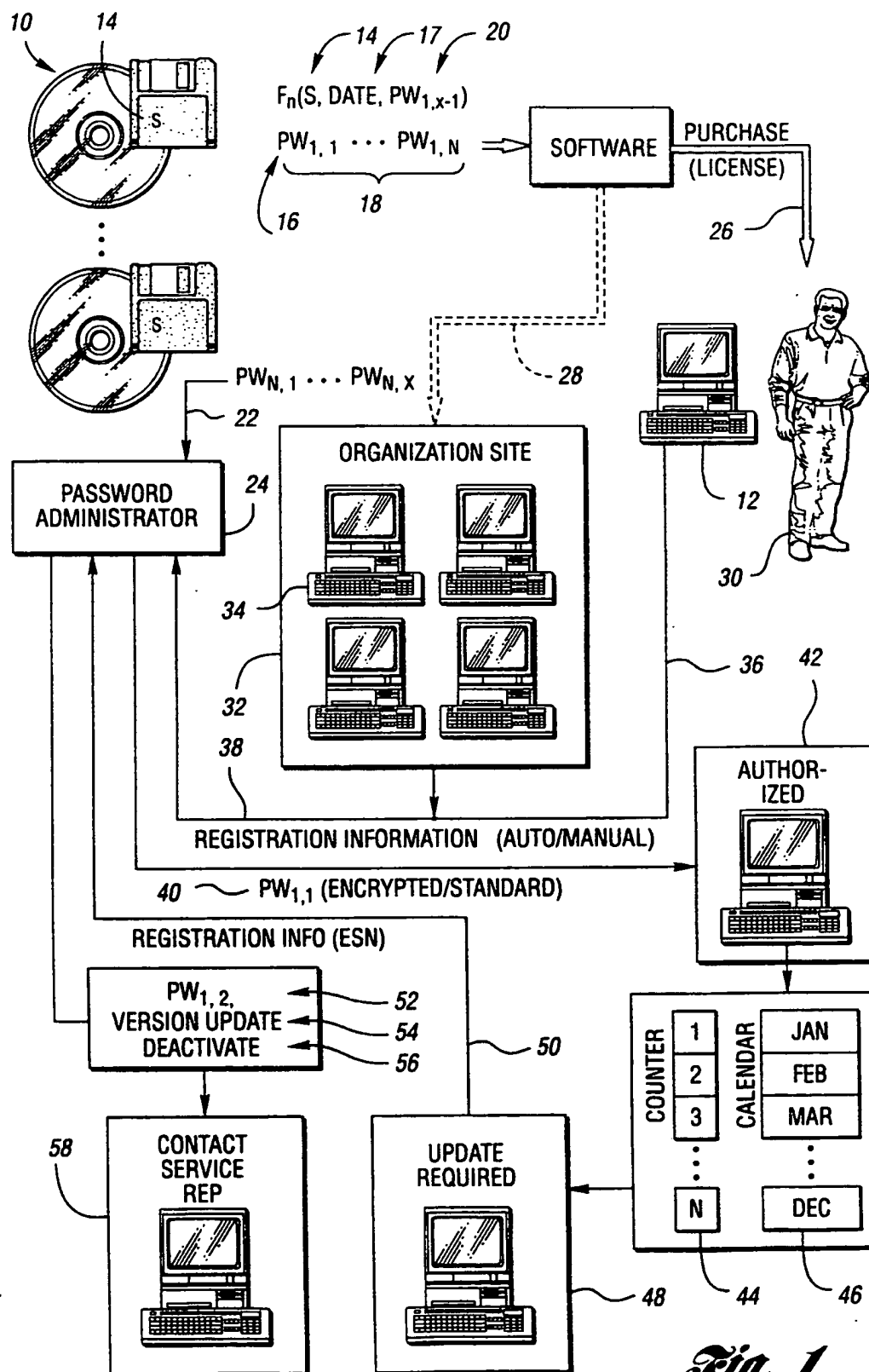
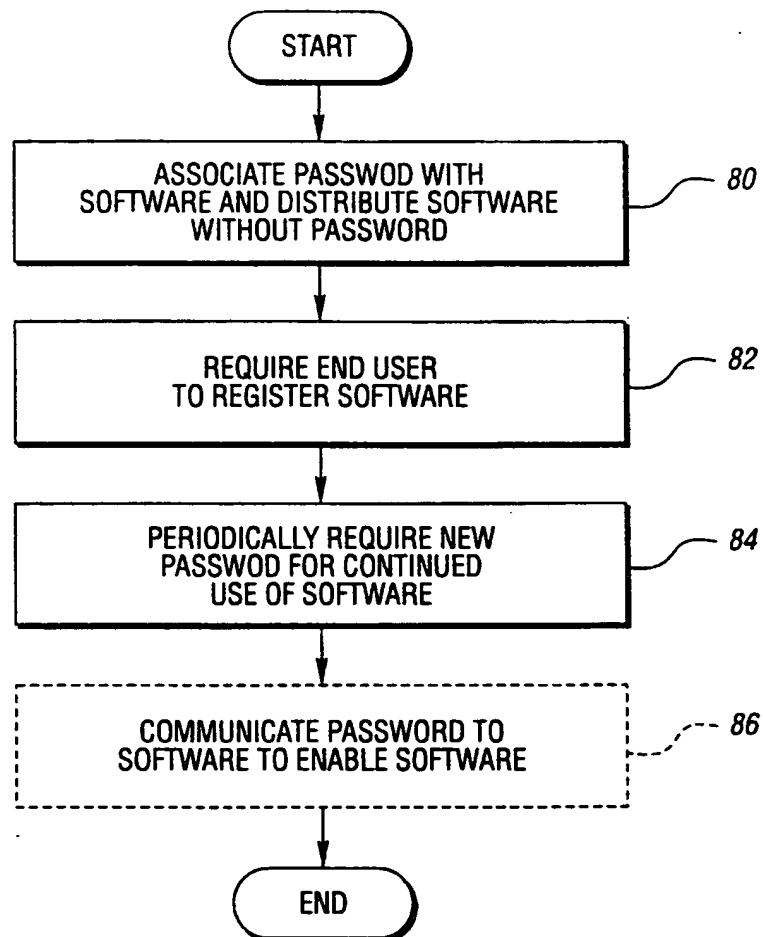


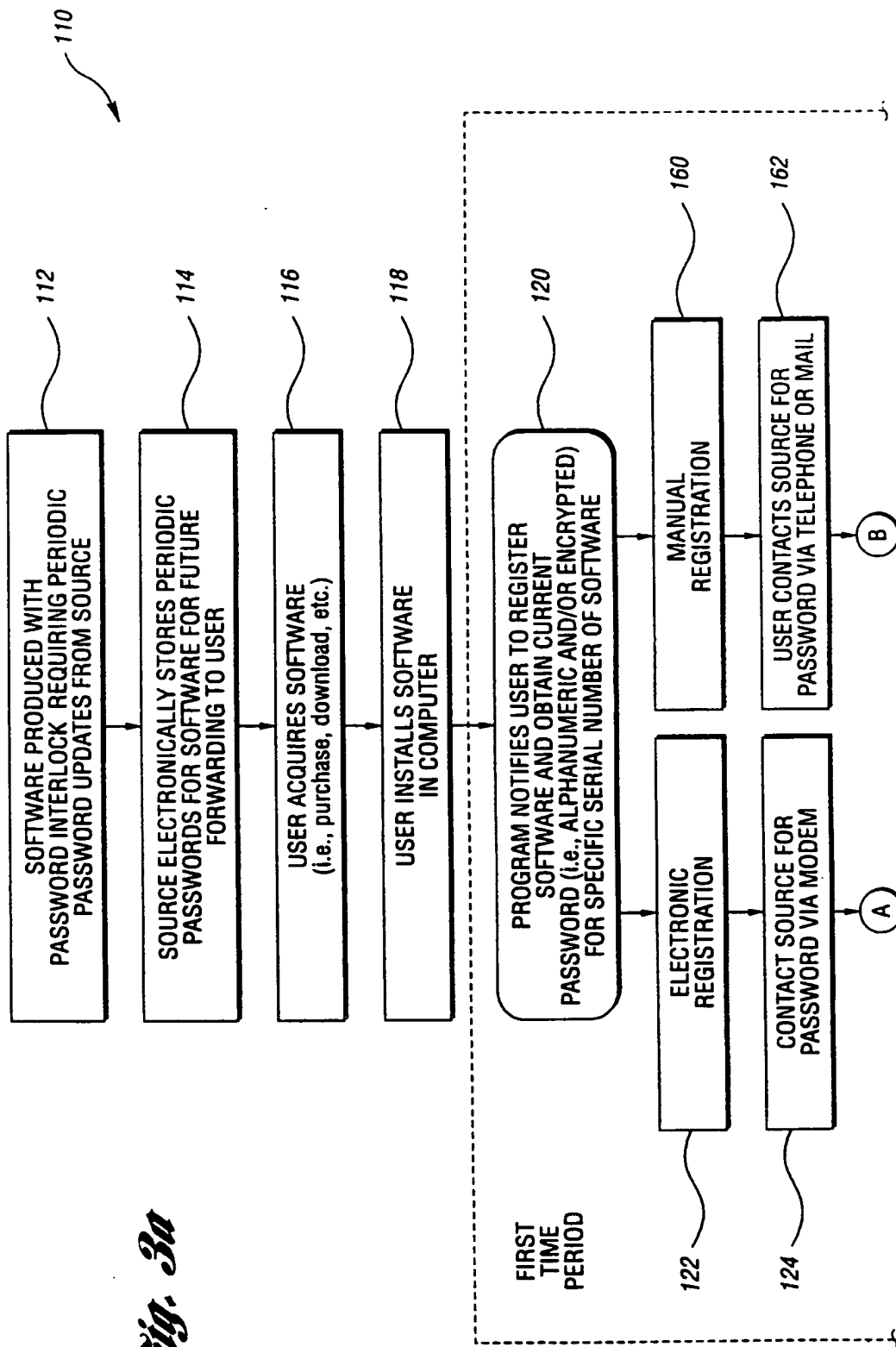
Fig. 1

2/6

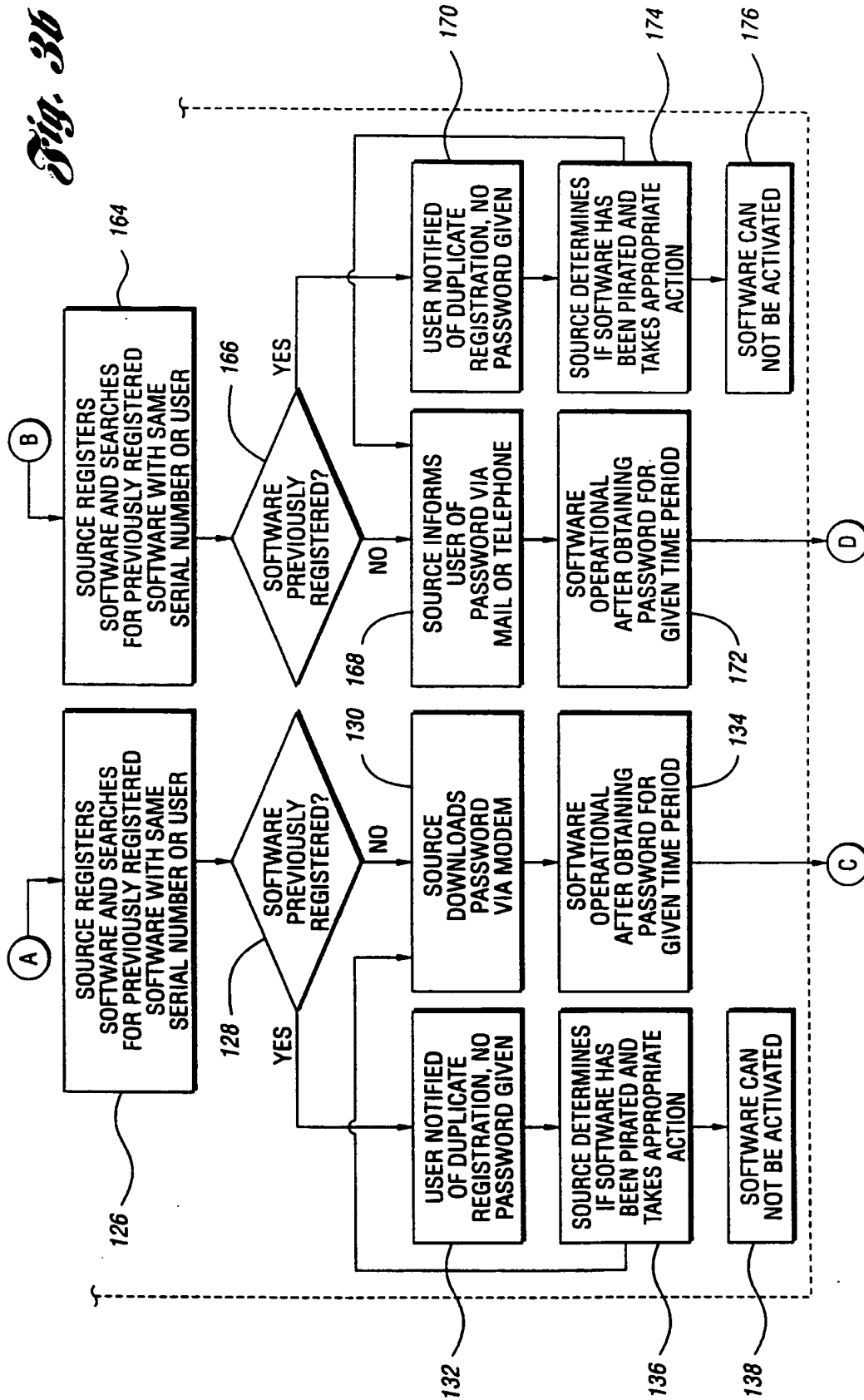
*Fig. 2*



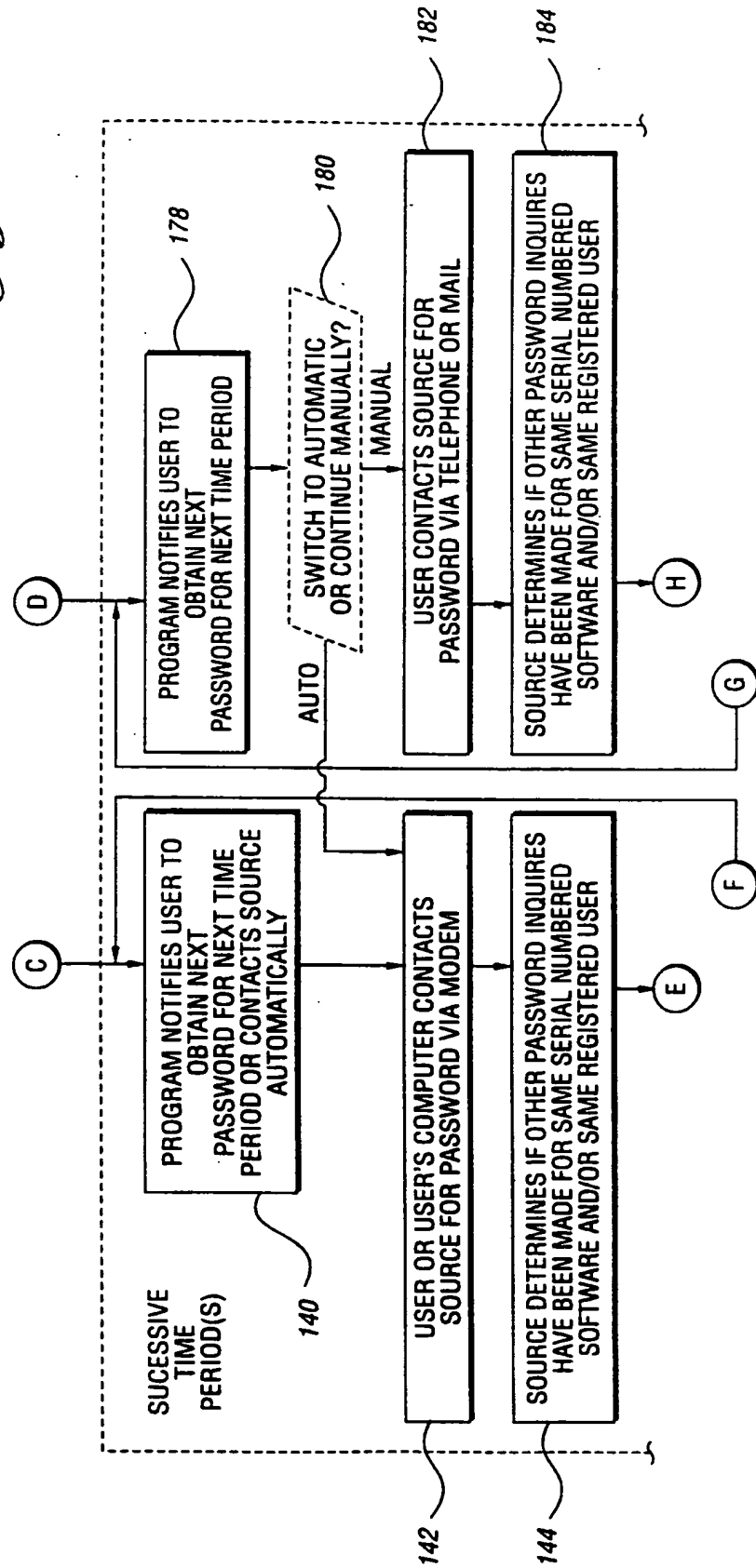
*Fig. 3a*



4/6

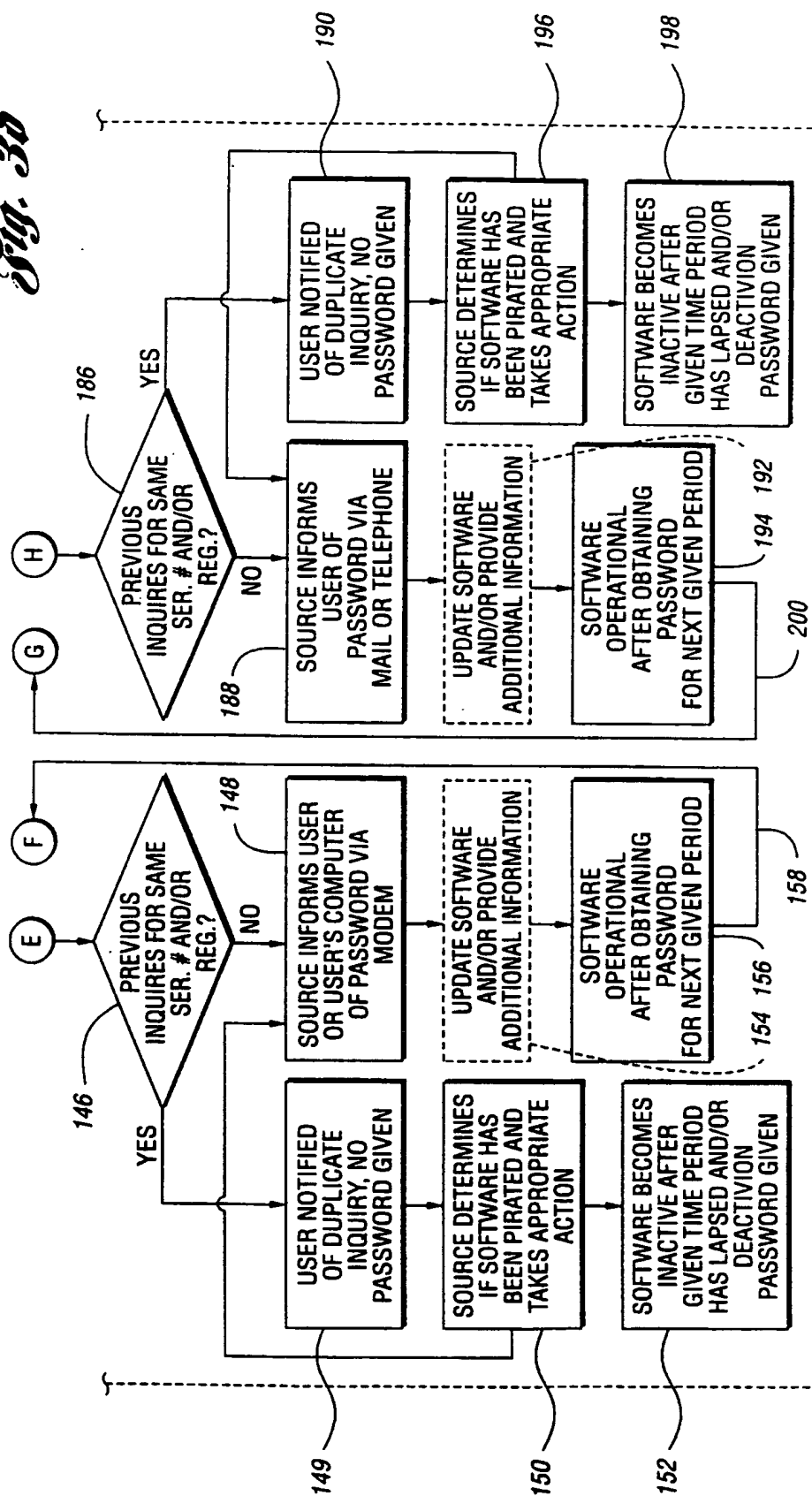


5/6

*Fig. 3c*

6/6

Fig. 3b



## INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US99/11647

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC(6) : H04L 09/00, 09/06 US CL : 713/200, 201, 202; 709/229; 380/3, 4, 23 According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) U.S. : 713/200, 201, 202; 709/229; 380/3, 4, 23 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) Please See Extra Sheet.		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,652,793 A (PRIEM ET AL) 29 JULY 1997, COL 1, LINES 65-67, COL 3 TO COL 6	10-12,31 --- 1 - 7 , 9 , 13 - 18,32,37,40-4 4
X --- Y	US 5,509,070 A (SCHULL) 16 APRIL 1996, COL 1, LINES 52-65, COL 5, LINES 59-67, COL 6, LINES 1-12, COL 8, LINES 55-58, COL 9, LINES 58-65, COL 10, LINES 16-25, COL 17, LINES 46-67, COL 20, LINES 29-33	38 --- 1 , 2 , 7 , 9 , 13 - 18,32,40,4 1
X	US 5,579,479 A (PLUM) 26 NOVEMBER 1996 COL 7, LINES 38-56	39
Y,P	US 5,842,124 A (KENAGY ET AL) 24 NOVEMBER 1998 COL 2, COL 7, LINES 57-67, COL 8, LINES 1-45, COL 10, LINES 58-60, COL 11, LINES 33-45	2,18,37,42,45
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "G" document member of the same patent family	
Date of the actual completion of the international search 28 JULY 1999		Date of mailing of the international search report 24 AUG 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230		Authorized officer CHRISTOPHER R. MATTHEWS Telephone No. (703) 305-9600

# INTERNATIONAL SEARCH REPORT

International application No.  
PCT/US99/11647

## B FIELDS SEARCHED

Electronic data bases consulted (Name of data base and where practicable terms used):

APS, JPO, EPO, IEEE Electronic Library, NonPatent Literature

search terms: request, require, desire, ask, password, software, application, representative, developer, issuer,  
administrator, distributor, initial, enable, activate, series, multiple, additioanl, partial, plurality, temporary, multiple, trial,  
limited, license, registration, protected